IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Robert Rice et al.
Serial No.:	10/784,708
Filing Date:	February 23, 2004
Title:	Electronic Notary Service
Examiner:	Carlton Johnson
Art Unit:	2136
Confirmation No.:	1463

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P O Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF

This brief is in furtherance of the Notice of Appeal, filed in this case on May 1, 2008.

The fees required under § 1.17(c), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying Transmittal of Appeal Brief.

I. REAL PARTY IN INTEREST

The real parties in interest in this appeal are the following parties: Robert Rice and Jason Streit.

II. RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

III. STATUS OF CLAIMS

A. **TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1-2, 4-11, 13-18 and 21-24.

B. **STATUS OF ALL THE CLAIMS IN APPLICATION**

1. Claims pending: 1-2, 4-11, 13-18 and 21-24.
2. Claims previously cancelled: 3, 12, 19 and 20.
3. Claims withdrawn: None.
4. Claims rejected: 1-2, 4-11, 13-18 and 21-24.
5. Claims allowed: None.
6. Claims cancelled in accompanying amendment: None.

C. **CLAIMS ON APPEAL**

The claims on appeal are: 1-2, 4-11, 13-18 and 21-24.

IV. STATUS OF AMENDMENTS

No amendments were filed after final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention as recited in independent claim 1 provides a method for notarizing and verifying documents via a distributed computer network.[1] While the general concept of notarization crosses legal jurisdictions, each jurisdiction has its own unique, local requirements for proper notarization.[2] A problem often encountered with notarization of legal documents is geographic distance between parties to a document.[3] In such a scenario, the documents must be physically sent to one party, who signs them and has them notarized by a local notary in accordance with local legal requirements.[4] This process is cumbersome and time consuming and also runs the risk of losing documents while sending them back and forth.[5]

The present invention involves creating an electronic version of the document on a client computer in the network, which is then encrypted and stored on a secure server in the computer network, wherein the stored electronic document may be retrieved by any client in the computer network.[6] The electronic document includes an acceptance option for a Consent to Electronic Records (CER).[7] The signing party is then notified of the electronic document's identity and directed to the location of a certified notary within the signing party's geographic vicinity.[8] The signing party visits the notary and retrieves the electronic document on the notary's client computer and is presented with the CER.[9] If the signor accepts the CER the signer reviews and signs the document electronically, e.g., with an electronic signature pad.[10] The notary verifies the transaction and electronically affixes an official notary seal to the electronic document using a notary application that stores the electronic seal.[11] The signed, notarized document is saved and any certified notary in the network may then retrieve the signed, notarized document.[12]

---

[1] Application, page 3, lines 3-4.
[2] Application, page 2, lines 11-13.
[3] Application, page 2, lines 16-17.
[4] Application, page 2, lines 17-19.
[5] Application, page 2, lines 21-22.
[6] Application, page 3, lines 4-7.
[7] Application, page 8, lines 17-18.
[8] Application, page 3, lines 7-9.
[9] Application, page 9, lines 1-6.
[10] Application, page 9, lines 7-11.
[11] Application, page 9, lines 14-17.

The present invention as recited in independent claim 11 provides a system for notarizing and verifying documents via a distributed computer network.[13] The system includes means for creating an electronic version of the document on a client computer in the network, which is then encrypted and stored on a secure server in the computer network, wherein the stored electronic document may be retrieved by any client in the computer network.[14] The electronic document includes an acceptance option for a Consent to Electronic Records (CER).[15] The signing party is then notified of the electronic document's identity and directed to the location of a certified notary within the signing party's geographic vicinity.[16] The signing party visits the notary and retrieves the electronic document on the notary's client computer and is presented with the CER.[17] If the signor accepts the CER the signer reviews and signs the document electronically, e.g., with an electronic signature pad.[18] The notary verifies the transaction and electronically affixes an official notary seal to the electronic document using a notary application that stores the electronic seal.[19] The signed, notarized document is saved and any certified notary in the network may then retrieve the signed, notarized document.[20]

The present invention as recited in independent claim 18 provides a computer program product for notarizing and verifying documents via a distributed computer network.[21] The program product includes instructions for creating an electronic version of the document on a client computer in the network, which is then encrypted and stored on a secure server in the computer network, wherein the stored electronic document may be retrieved by any client in the computer network.[22] The electronic document includes an acceptance option for a Consent to Electronic Records (CER).[23] The signing party is then notified of the electronic document's identity and directed to the location of a

---

[12] Application, page 3, lines 13-14.
[13] Application, page 3, lines 3-4.
[14] Application, page 3, lines 4-7.
[15] Application, page 8, lines 17-18.
[16] Application, page 3, lines 7-9.
[17] Application, page 9, lines 1-6.
[18] Application, page 9, lines 7-11.
[19] Application, page 9, lines 14-17.
[20] Application, page 3, lines 13-14.
[21] Application, page 3, lines 3-4.
[22] Application, page 3, lines 4-7.

certified notary within the signing party's geographic vicinity.[24] The signing party visits the notary and retrieves the electronic document on the notary's client computer and is presented with the CER.[25] If the signor accepts the CER the signer reviews and signs the document electronically, e.g., with an electronic signature pad.[26] The notary verifies the transaction and electronically affixes an official notary seal that is stored by the computer program product to the electronic document.[27] The signed, notarized document is saved and any certified notary in the network may then retrieve the signed, notarized document.[28]

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 2, 4-11, 13-18, and 21-24 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Nassiri (US Pub. No. 2002/0143711).

VII. ARGUMENTS

REJECTION OF CLAIMS 1, 2, 4-11, 13-18 AND 21-24 UNDER 35 U.S.C. 103(a)

Prior to discussing the specific claims under appeal, we shall look first at the final rejection. With regard to the rejection of claims 1, 11 and 18, the Examiner writes:

> **Regarding Claims 1, 11, 18**, Nassiri discloses a method, system, computer program product in a computer readable medium for verifying a document via a distributed computer network, the method comprising the steps of:
>
> (b) storing the electronic document on a server in the computer network; (see Nassiri paragraph [0081], lines 2-27; paragraph [0080], lines 1-5: upload, download, store electronic document on host system (i.e. server))

---

[23] Application, page 8, lines 17-18.
[24] Application, page 3, lines 7-9.
[25] Application, page 9, lines 1-6.
[26] Application, page 9, lines 7-11.
[27] Application, page 9, lines 14-17.
[28] Application, page 3, lines 13-14.

(c) retrieving the electronic document using a notary application via a second client in the computer network; (see Nassiri paragraph [0080], lines 1-5: download (i.e. retrieve) electronic document)
(f) electronically affixing a verifying party's signature and seal to the electronic document using said notary application via the second client, wherein said seal is stored electronically by said notary application, and wherein the verifying party may be any certified party that has authority by law to verify and authenticate the signer of a document; (see Nassiri paragraph [0095], lines 1-6: attach notary digital signature, notary seal for notary public to electronic document; paragraph [0096], lines 4-10; paragraph [00970], lines 24-28: seal function embedded within the computer system, seal function cannot operate without notary application (distributed application)) and
(g) storing the signed, notarized, electronic document on said server. (see Nassiri paragraph [0102], lines 5-9: upload signed, notarized electronic document to host system (i.e. server))

Claim 1 of the present application recites:

1. A method for verifying a document via a distributed computer network, the method comprising the steps of:

(a) creating an electronic version of the document on a first client in the computer network, wherein said electronic document includes an acceptance option for a Consent to Electronic Records (CER);

(b) storing the electronic document on a server in the computer network;

(c) retrieving the electronic document using a notary application via a second client in the computer network;

(d) presenting a signing party with said acceptance option for said CER;

(e) electronically affixing at least one signing party's signature to the electronic document using said notary application via the second client only if said signing party accepts the CER;

(f) electronically affixing a verifying party's signature and seal to the electronic document using said notary application via the second client, wherein said seal is stored electronically by said notary application, and wherein the verifying party may be any certified party that has authority by law to verify and authenticate the signer of a document; and

(g) storing the signed, notarized, electronic document on said server.

For the purposes of the present discussion, claims 11 and 18 recite similar limitations.

The manner in which Nassiri stores and applies the notary seal differs from the approach used in the present invention. Nassiri employs a notary seal input device that is

independent from the desktop manager application used to perform the notarization function. In the preferred embodiment of Nassiri, the notary seal input device is a portable hardware device that is separate from the computer system running the desktop manager. Nassiri briefly mentions that the notary seal input device may also be a function imbedded in the local computer system. However, the notary input device is always described as a separate entity from the desktop manager, with both entities being dependent upon each other to function. Specifically, Nassiri teaches:

> [0096] The electronic notary seal input device 90 is a device that is independent of the desktop manager 30 but nonetheless operates only in conjunction with the desktop manager's 30 notarization function. Likewise, the desktop manager's 30 notarization function only operates when activated by the electronic notary seal input device 90. The electronic notary seal input device 90 may be a function embedded in the customer local computer system 20 or a portable device that attaches to the customer local computer system 20. The electronic notary seal function 115 will only operate in conjunction with the notary seal input device 90 verifying the credentials of the notary public 100 in the host computer system 40 registration database. As stated, verification information consists of that information required by law to license and register with a respective state as a notary public.
>
> [0097] In the preferred embodiment pf the present invention, the electronic notary seal input device 90 is a remote hardware device that remains in the sole possession of the notary public 100. The notarization function of the desktop manager 30 will only run when the electronic notary seal input device 90 is attached to the notary public 100 customer local computer system 20. The remote electronic notary seal input device 90 is a hardware-based security portable device that attaches to the serial or parallel printer port of the notary public 100 customer local computer system 20, including a portable laptop of the traveling notary public 100. The remote electronic notary seal input device 90 utilizes a hardware key that uses codes and passwords embedded inside the key to control access to the desktop manager's 30 notarization function. While activated, the electronic notary seal input device 90 receives encoded data from the desktop manager 30 an decodes it in a way that cannot be imitated. The decode data that is returned from the remote electronic notary seal input device 90 is deployed in the desktop manager 30 so that it affects the mode in which the desktop manager 30 executes the notarization function 110. The remote electronic notary seal input device 90 is programmed to execute a notarization 110 upon a verified match with the desktop manager 30. After decoding, a verified match executes the notarization function of the desktop manage 30 that in turn activates the execution of

> the electronic notary seal 115 which is embedded in the remote electronic notary seal input device 90.

In the present invention, the seal is stored by the notary software application itself. A great advantage of the present invention is that all functions of storing and applying the seal are bundled together in the same software package that is used to execute the other notarization functions. Nassiri does not teach this and in fact teaches in the opposite direction by placing great emphasis on keeping the notary seal input device separate from the desktop manager application.

The Examiner's argument incorrectly conflates the software application with hardware, which is a critical distinction. The paragraphs cited by the Examiner (quoted above) quite clearly stipulate that the electronic notary seal used by the Nassiri invention is implemented in hardware, either as a remote hardware device (in the preferred embodiment) or imbedded in the computer hardware itself. Furthermore, Nassiri is also very clear that the notary seal device is supposed to be independent of the desktop manager, teaching away from the present invention. Therefore, unlike the present invention, the electronic notary seal in Nassiri is not part of the software application.

The Examiner points to the fact that the electronic seal and notary software application in Nassiri need each other to function. However, this merely reinforces the fact that the notary seal and software are separate elements that have to be brought together, unlike the present invention which has the seal itself incorporated into the software application.

Furthermore, Nassiri does not teach or suggest adding an acceptance option for a Consent to Electronic Records (CER) to the electronic document and requiring a CER from a signer before allowing the document to be executed. This omission by Nassiri could have serious legal consequences depending on the jurisdiction in question.

With regard to the Consent to Records feature of the claimed invention, the Examiner writes:

> The disclosure of an option for "Consent to Electronic Records" is well known in the art. A consumer (client) has to consent to not receive a paper copy of a transaction in lieu of access to an electronic copy of such a transaction. The capability to give a consumer (client) the right or option

> for acceptance or denial of access to transaction information in electronic form is well known in the art.
>
> ...The Nassiri prior art discloses that the consumer initiate the paperless transaction; therefore consent to operate within a paperless environment is implied. (See Nassiri paragraph [0076], lines 5-10: request to accept paperless (electronic) transaction information; paragraph [0020]: concern for legal requirements for transactions)

However, paragraph [0076] in Nassiri does not refer to a request for consent but rather to a request signature verification:

> [0076] With reference to FIG. 1, a customer 5 with internet or TCP/IP connectivity 10 may either a website, a local access network (LAN) or a wide access network (WAN) using a client-server infrastructure, to provide the point of access to the present invention. In the preferred embodiment of the present invention, the request for signature verification using a paperless document platform is initiated by the customer 5 accessing a website on the world-wide-web using the customer local computer system 20. The website provides the customer 5 with information about the services available and information in the form of a tutorial on how to register with, and use the present invention. Alternatively, the invention may be configured for use an a restricted LAN or a restricted WAN.

There is no mention of Consent to Eletronic Records anywhere in Nassiri. Applicant does agree that some type of consent could be reasonably implied in the operation of the Nassiri invention. However, even assuming *arguendo* that Nassiri does use some type of request for consent from a user, this does not necessarily result in the limitations recited in the claims.

Claims 1, 11, and 18 do not merely include the use of a CER but explicitly recite that the CER function is incorporated into the electronic document itself. This specific implementation is not suggested anywhere in Nassiri. Because Nassiri does not explicitly address the issue of Consent to Electronic Records, there is no guidance in Nassiri as to the specifics of how such a CER would be implemented in the system. For example, a CER could just as easily be incorporated into the operation of the notary software application rather than the electronic document itself. Alternatively, it might be implemented in the operating system of the computer hosting the notary application.

Therefore, the specific limitation of incorporating the CER into the electronic document itself is not obvious in light of either the current art in general or the Nassiri reference.

Therefore, it is respectfully asserted that the Nassiri reference does not teach all of the limitations of the claimed invention, nor are the specific limitations of the present invention obvious in view of Nassiri.

Because claims 2, 4-10, 13-17, and 21-24 depend from claims 1, 11 and 8, respectively, they are distinguished from Ballester and Evans for the reasons explained above.

In view of the above, Applicant respectfully submits that the rejection of claims 1, 2, 4-11, 13-18, and 21-24 is overcome and should not be sustained.

CONCLUSION

In view of the above arguments, Appellant respectfully submits that all the extant claims are allowable over the cited prior art and that the application is in condition for allowance. Accordingly, Appellant respectfully requests the Board of Patent Appeals and Interferences to overturn the rejections set forth in the Final Office Action.

Respectfully submitted,

Dated: June 3, 2008

By: Christopher P. O'Hagan

Christopher P. O'Hagan
Registration No. 46,966
Attorney for Applicant

CARSTENS & CAHOON, LLP
PO Box 802334
Dallas, TX 75380
(972) 367-2001 *Telephone*
(972) 367-2002 *Facsimile*

VIII. APPENDIX OF CLAIMS ON APPEAL

1. A method for verifying a document via a distributed computer network, the method comprising the steps of:

(a) creating an electronic version of the document on a first client in the computer network, wherein said electronic document includes an acceptance option for a Consent to Electronic Records (CER);

(b) storing the electronic document on a server in the computer network;

(c) retrieving the electronic document using a notary application via a second client in the computer network;

(d) presenting a signing party with said acceptance option for said CER;

(e) electronically affixing at least one signing party's signature to the electronic document using said notary application via the second client only if said signing party accepts the CER;

(f) electronically affixing a verifying party's signature and seal to the electronic document using said notary application via the second client, wherein said seal is stored electronically by said notary application, and wherein the verifying party may be any certified party that has authority by law to verify and authenticate the signer of a document; and

(g) storing the signed, notarized, electronic document on said server.

2. The method according to claim 1, wherein the verifying party in step (e) is a notary.

4. The method according to claim 1, wherein the seal is stored electronically in the notary application on the second client.

5. The method according to claim 1, wherein the verifying party's signature is stored on the second client.

6. The method according to claim 1, wherein the signing party is provided with the location of an authorized verifying party nearest to the signing party's geographic location.

7. The method according to claim 1, further comprising:

creating and updating an electronic journal file containing information regarding the verification transaction, wherein said file is stored in a journal database for the verifying party.

8. The method according to claim 7, wherein the information stored in the journal file may include:

sending party;
time;
dates;
type of document;
fees;
type of notarization;
signer's signature; and
verification information.

9. The method according to claim 1, wherein an authorized verifying party can both create the electronic document and verify the electronic document.

10. The method according to claim 1, wherein a certified creator can only create the electronic document.

11. A system for verifying a document via a distributed computer network, the system comprising:

(a) means for creating an electronic version of the document on a first client in the computer network, wherein said electronic document includes an acceptance option for a Consent to Electronic Records (CER);

(b) means for storing the electronic document on a server in the computer network;

(c) means for retrieving the electronic document using a notary application via a second client in the computer network, using a notary application;

(d) means for presenting a signing party with said acceptance option for a CER;

(e) means for electronically affixing at least one signing party's signature to the electronic document using said notary application via the second client only if said signing party accepts the CER;

(f) means for electronically affixing a verifying party's signature and seal to the electronic document using said notary application via the second client, wherein said seal is stored electronically by said notary application, and wherein the verifying party may be any certified party that has authority by law to verify and authenticate the signer of a document; and

(g) means for storing the signed, notarized, electronic document on said server.

13. The system according to claim 11, wherein the seal is stored electronically in the notary application on the second client.

14. The system according to claim 11, wherein the verifying party's signature is stored on the second client.

15. The system according to claim 11, further comprising:

an electronic journal file containing information regarding the verification transaction, wherein said file is stored in a journal database for the verifying party.

16. The system according to claim 15, wherein the information stored in the journal file may include:

sending party;

time;

dates;

type of document;

fees;

type of notarization;

signer's signature; and

verification information.

17. The system according to claim 11, further comprising means for providing the signing part with the location of an authorized verifying party nearest to the signing party's geographic location

18. A computer program product in a computer readable medium, for verifying a document via a distributed computer network, the computer program product comprising:

(a) first instructions for creating an electronic version of the document, wherein said electronic document includes an acceptance option for a Consent to Electronic Records (CER);

(b) second instructions for storing the electronic document on a server in the computer network;

(c) third instructions for retrieving the electronic document from said server;

(d) fourth instructions for presenting a signing party with said acceptance option for a CER;

(e) fifth instructions for electronically affixing at least one signing party's signature to the electronic document only if said signing party accepts the CER;

(f) sixth instructions for electronically affixing a verifying party's signature and seal to the electronic document, wherein said seal is stored electronically by the computer program, and wherein the authorized user may be any certified party that has authority by law to verify and authenticate the signer of a document; and

(f) sixth instructions for storing the signed, notarized, electronic document on said server.

21. The computer program product according to claim 18, wherein the verifying party's signature is stored by the computer program.

22. The computer program product according to claim 18, further comprising instructions for providing the signing party with the location of an authorized verifying party nearest to the signing party's geographic location.

23. The computer program product according to claim 18, further comprising:

an electronic journal file containing information regarding the verification transaction, wherein said file is stored in a journal database for the verifying party.

24. The computer program product according to claim 23, wherein the information stored in the journal file may include:

sending party;
time;
dates;
type of document;
fees;
type of notarization;
signer's signature; and
verification information.

APPENDIX OF EVIDENCE

No affidavits have been submit and relied upon by the Appellant under 37 CFR §§ 1.130, 1.131, or 1.132 in the pending appeal.

APPENDIX OF RELATED PROCEEDINGS

There have been no decisions rendered by a court or the Board in any proceeding pursuant to 37 CFR 41.37 (c)(1)(ii).